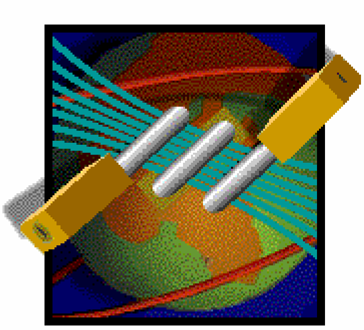


Cisco Secure ACS v4.0

中文简易使用手册

编著：邱 杨
qiuy.mail@gmail.com
福建富士通
2007-4-25

福富软件

目录

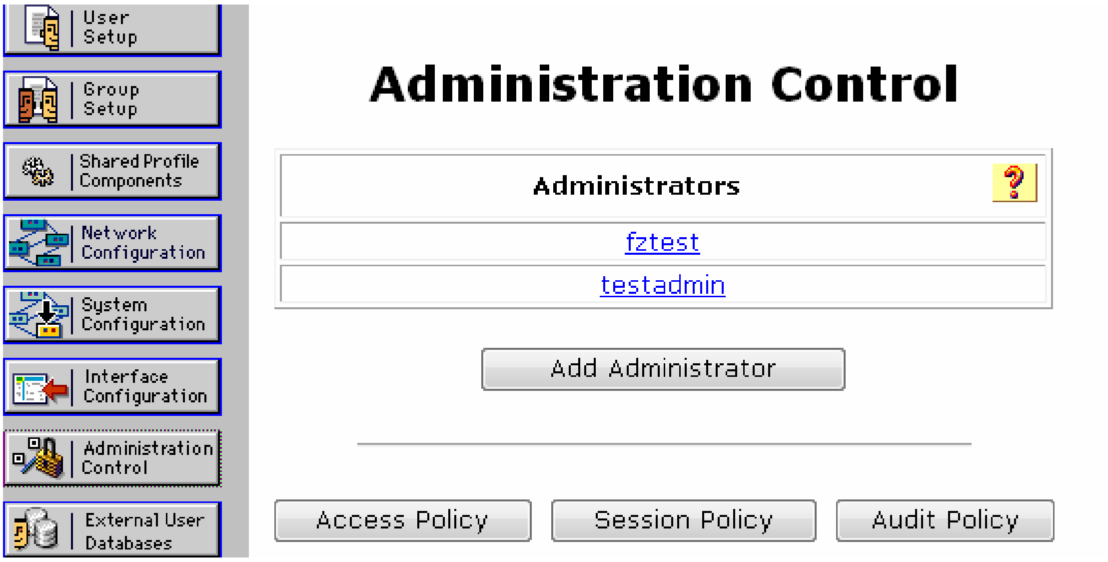
1.ACS基本配置..3
1.1 设置ACS管理员帐号..3
1.2 ACS网络设置（添加Tacacs+ 客户端） 4
1.3 Tacacs+设置..6
1.4 设备端tacacs+服务器的指定..7
2.ACS用户组/用户添加..7
2.1 添加用户组..7
2.2 添加用户..8
3.ACS功能设置..11
3.1 ACS认证(authentication)..11
3.2 ACS授权(authorization) 11
3.3 ACS审计(accounting)..14

1.ACS 基本配置

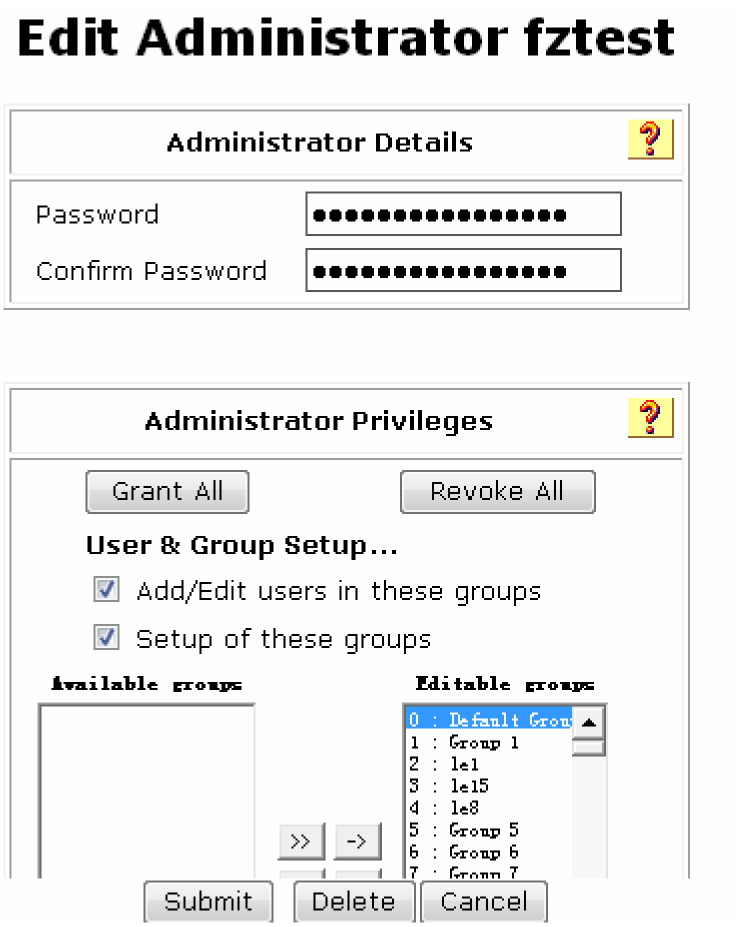
1.1 设置 ACS 管理员帐号

Step 1>点击 ACS 界面左边的 Administration control 按钮

，然后点击 Administrator control 界面中的 Add Administrator



Step 2>点击 Add administrator 后出现此账户的诸多选项，逐一填写后点击 Submit

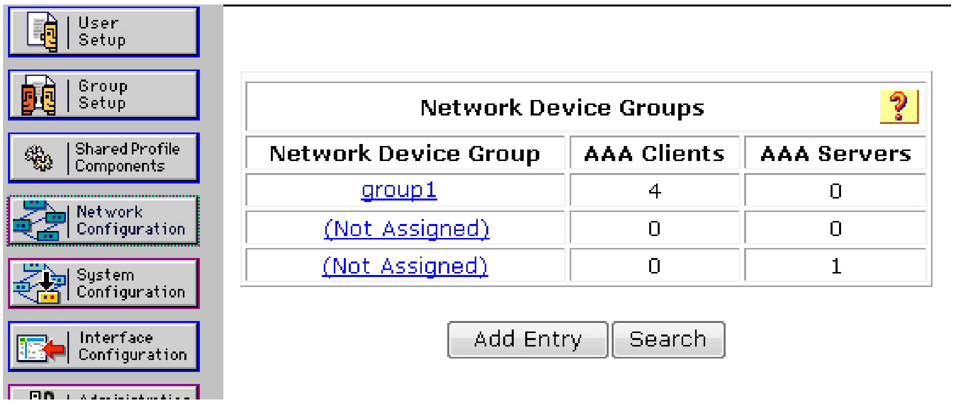


Step3>设置了管理员后就可以通过 web 界面登录到 ACS 服务器对 ACS 进行配置

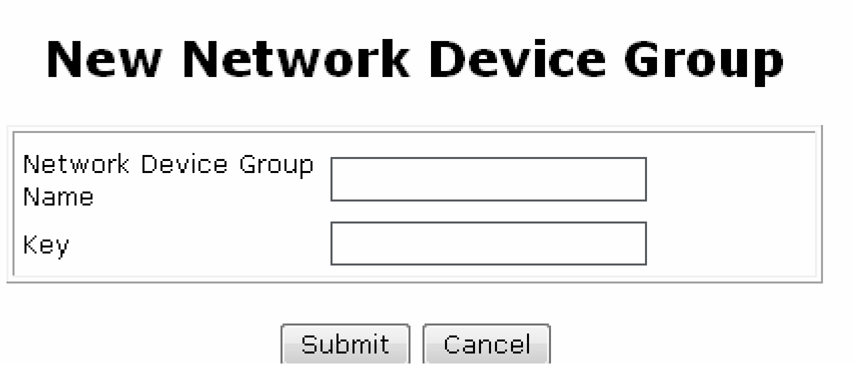
1.2 ACS 网络设置（添加 Tacacs+ 客户端）

Step1>点击 ACS 界面的 Network Configuration 按钮

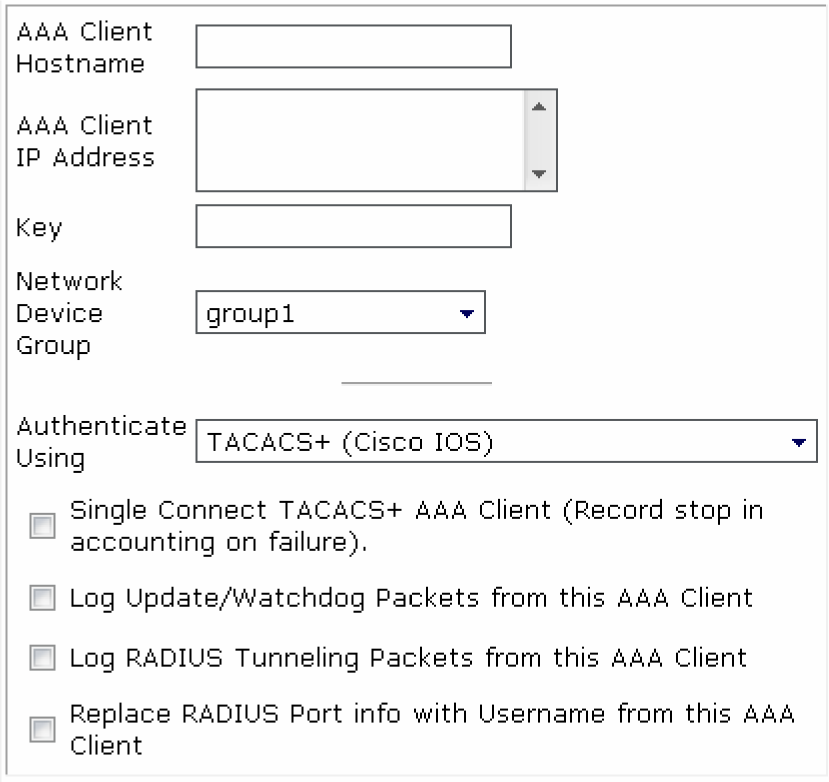
，出现网络配置界面，然后点击 Add Entry,



Step2>填写设备组的名称以及 key



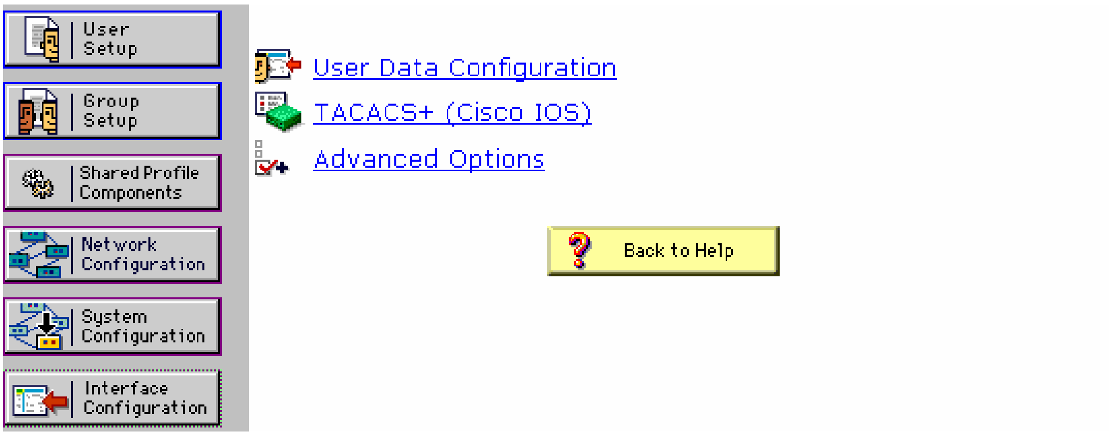
Step3>设备组定义了之后，点击此设备组属性就可以在此设备组中添加 Tacacs+客户端（ACS 中必须指定 Tacacs+客户端的 IP 地址）



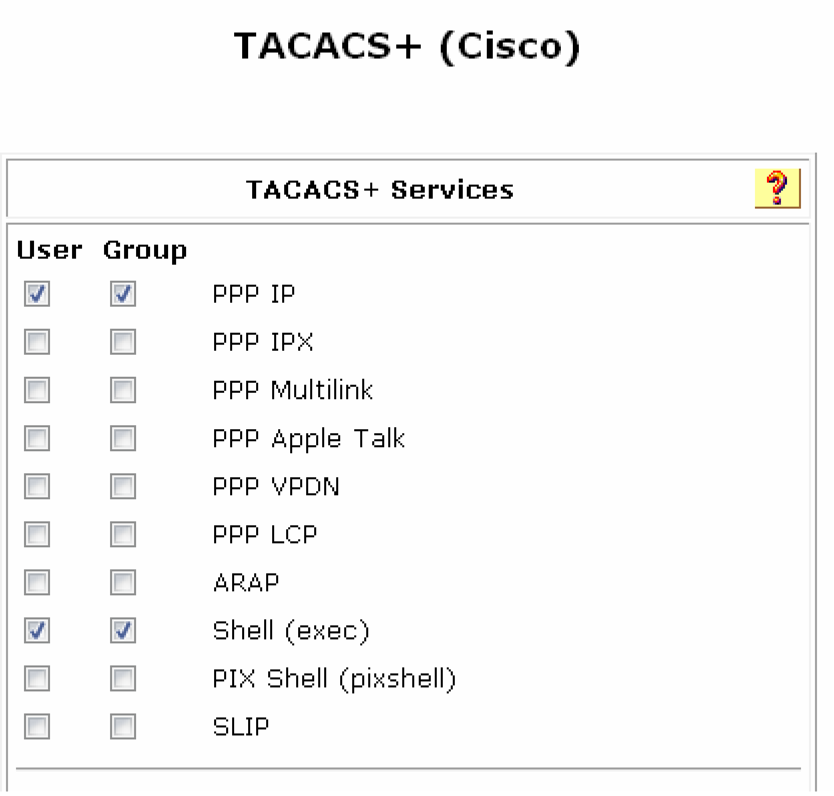
1.3 Tacacs+设置

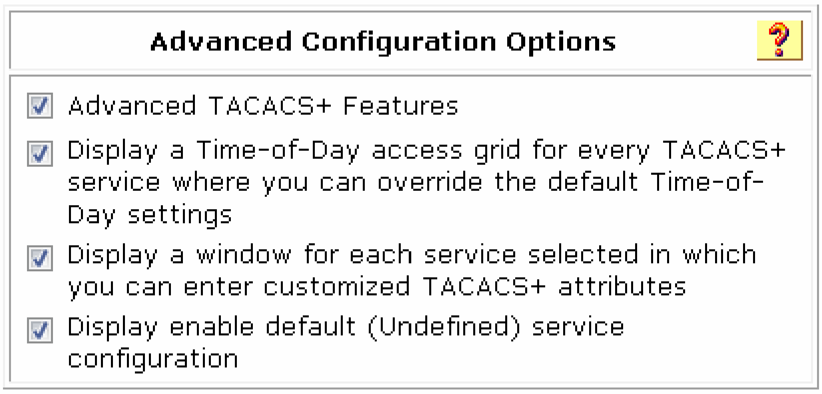
Step1>点击 ACS 界面左边 Interface configuration 按钮

，选择 TACACS+ (Cisco IOS)



Step2>根据个人具体应用，在 Tacacs+相关项目中打勾(如果没有将 tacacs+相关项目选中，则在用户组/用户属性中将不会出现 tacacs+相关项目)





1.4 设备端 tacacs+服务器的指定

在 cisco 设备端用以下命令指定 ACS tacacs+服务器

tacacs-server host 202.101.110.110

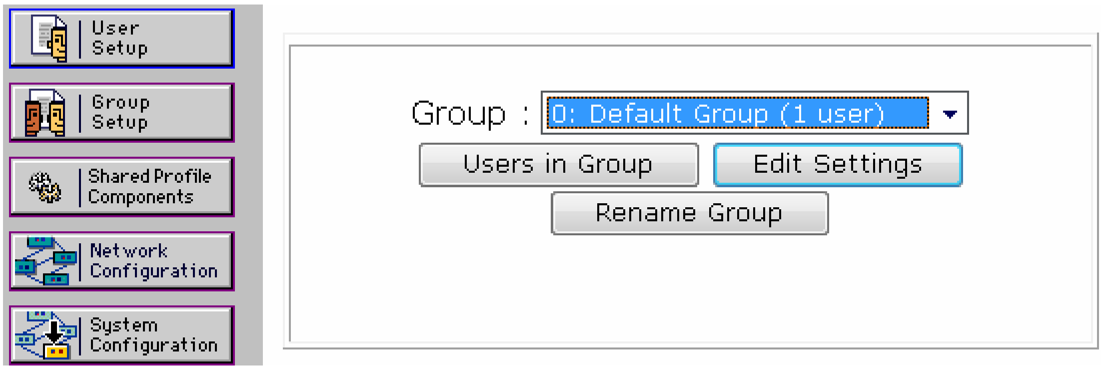
tacacs-server directed-request

tacacs-server key test

2.ACS 用户组/用户添加

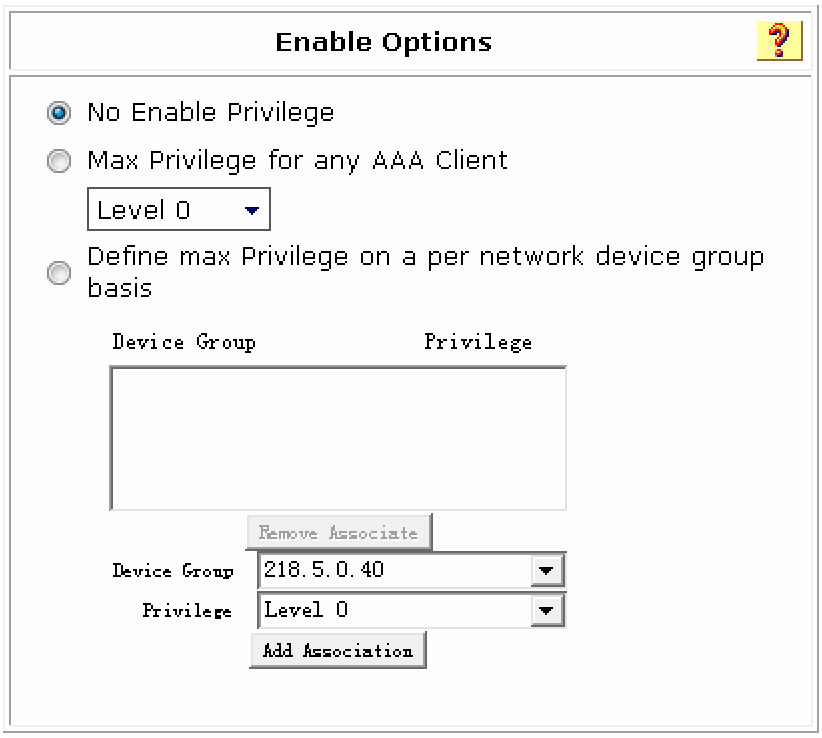
2.1 添加用户组

Step1>在 ACS 界面左边点击 Group Setup

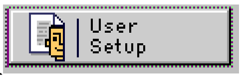


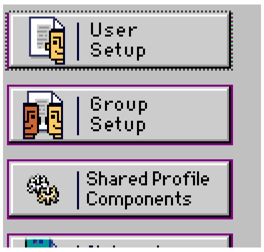
Step2>在下拉列表中选取某个组，给这个组重命名，接着选择 Edit setting 进入组的属性配置

Step3>在组的 enable option 中的 Max privilege for any AAA Client 设置组的级别



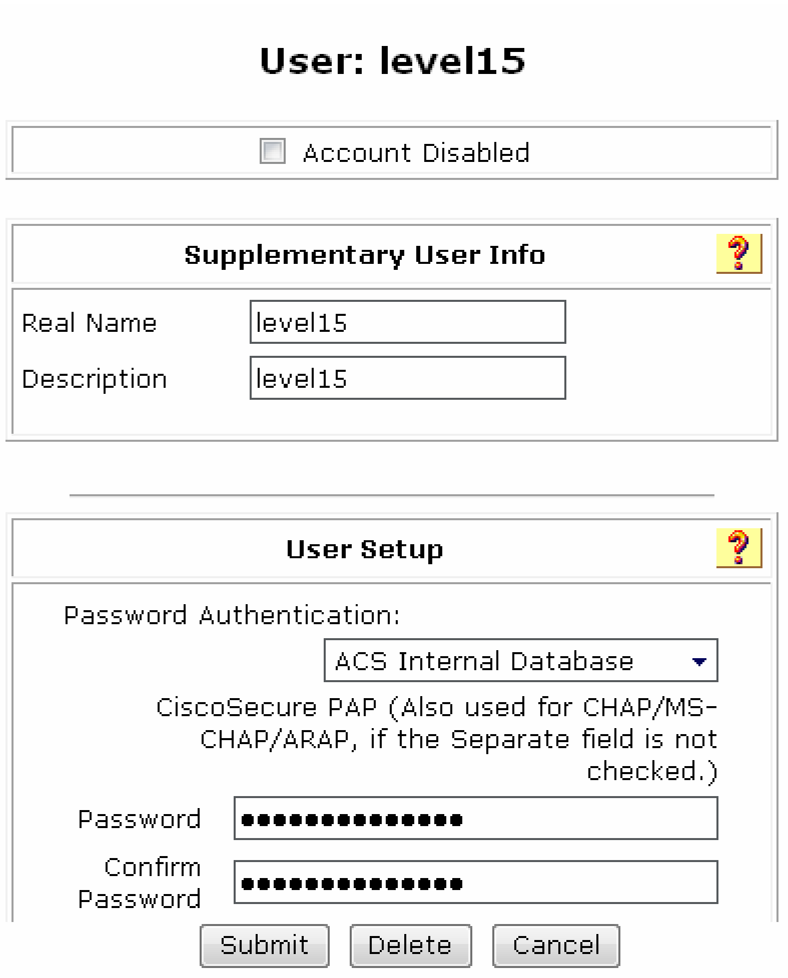
2.2 添加用户

Step1>在 ACS 界面的左边点击 user setup 按钮

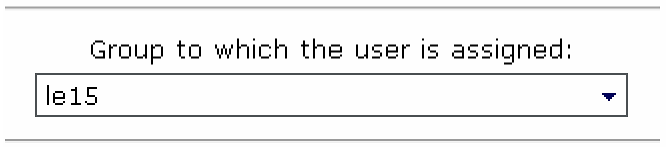


Step2>在 user 方框中填写用户名，然后点击 ADD/Edit

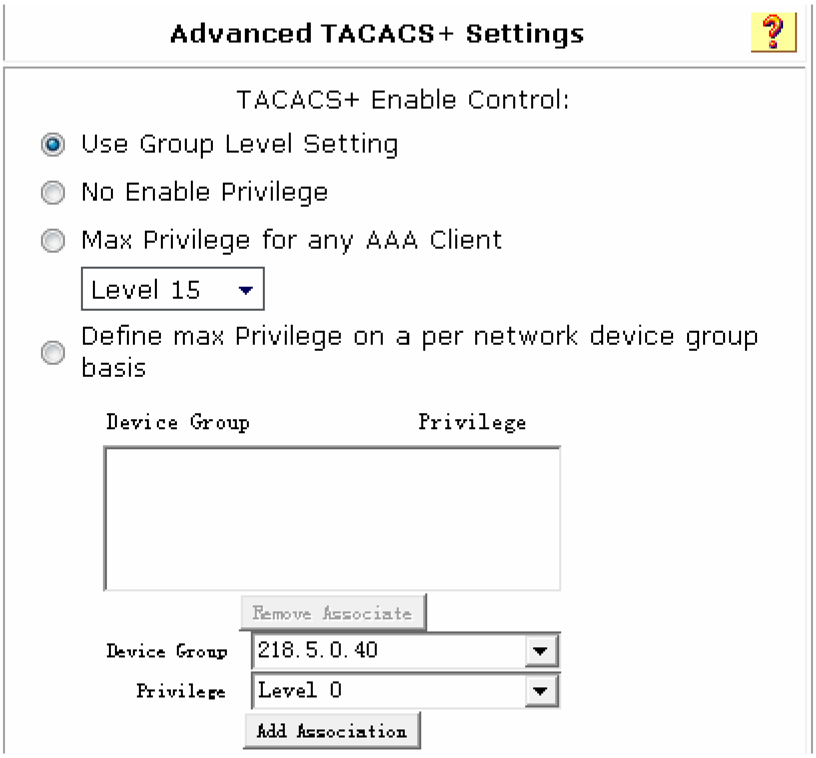
Step3>在出现的用户属性中逐一填写



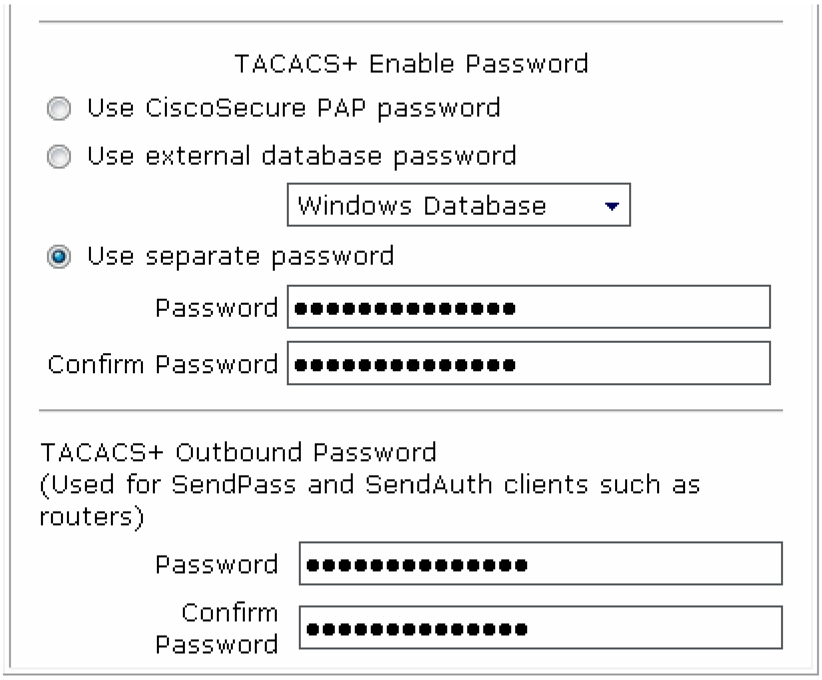
Step4>选择用户属于哪个用户组



Step5>选择用户属于的级别（可以定义单个用户级别，也可以和所属的用户组级别一样）



Step6>设置用户的 enable 密码



3.ACS 功能设置

3.1 ACS 认证(authentication)

Step1>在设备端定义 tacacs+服务器地址以及 key
tacacs-server host 202.101.110.110
tacacs-server directed-request
tacacs-server key test

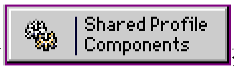
Step2>在 ACS 端定义设备的 IP 地址

Step3>在 ACS 上面建立用户名和用户组

Step4>在设备端配置 AAA 认证
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
line vty 0 4
login authentication default

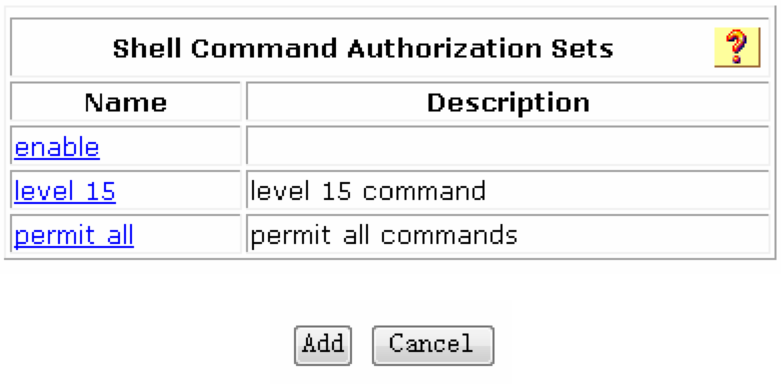
3.2 ACS 授权(authorization)

ACS 中可以通过设置用户组/用户的级别 privilege 来实现不同用户登录设备后可用的命令的不同，也可以通过使用 ACS 的命令授权来实现不同用户登录设备的可用命令条目，以下介绍 ACS 的命令授权。

Step1>在 ACS 的界面左边的

按钮

Step2>点击 shell command authorization sets



Shell Command Authorization Sets	
Name	Description
enable	
level 15	level 15 command
permit all	permit all commands

Add Cancel

Step3>点击 Add 添加命令集

页面下方有两个方框，左边填写命令的前缀，右边填写命令的后缀，命令后缀填写的语法格式是：permit/deny ***

以下是命令写法示例：

Command	Arguments
show	permit curpriv permit version permit aaa permit config
enable	*none*
disable	*none*

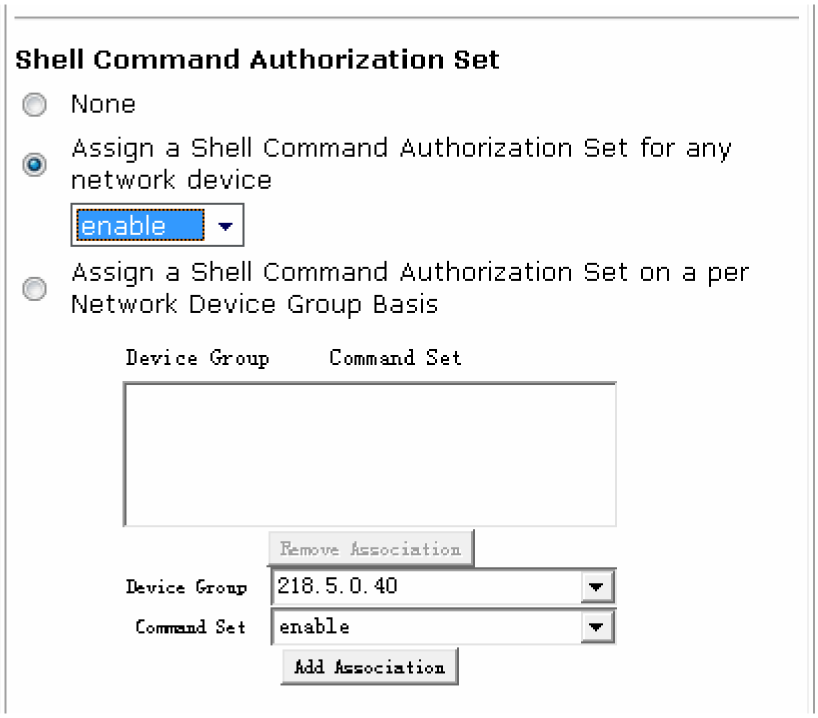
quit	*none*
login	*none*
logout	*none*
help	*none*

Step4>将命令集运用到用户组或者用户

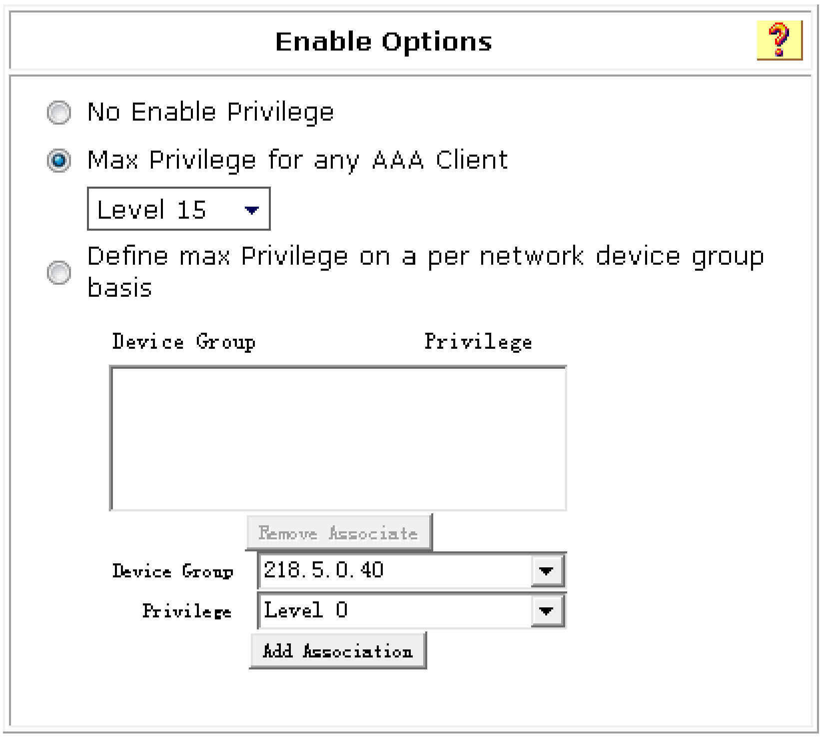
点击用户组属性的 tacacs+ setting 项目

将 shell(exec)选项打勾

在 Shell Command Authorization Set 属性中，选择 Assign a Shell Command Authorization Set for any network device，在下拉列表中选择刚才定义的的命令集



Step5>给用户组/用户的 enable 属性中选择用户组/用户的级别，然后点击 submit+restart



Step6>设备端配置

aaa new-model

aaa authorization commands 1 default group tacacs+ local

aaa authorization commands 15 default group tacacs+ local

line vty 0 4

authorization commands 1 default

authorization commands 15 default

3.3 ACS 审计(accounting)

Step1>设备端配置

aaa new-model

aaa accounting exec default start-stop group tacacs+

lin vty 0 4

accounting exec default

Step2>点击 ACS 界面左边的

按钮，然后选择 TACACS+ Accounting

Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts

可以具体浏览某一天的记录：

Date ↓	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed_time	service	bytes_in
04/23/2007	16:01:31	level1	le1	..	NAS Port re-used	3	..	..
04/23/2007	16:01:28	level1	le1	async	start	..	shell	..
04/23/2007	16:01:22	level1	le1	async	stop	185	shell	..
04/23/2007	15:58:20	level1	le1	..	NAS Port re-used	3	..	..
04/23/2007	15:58:17	level1	le1	async	start	..	shell	..
04/23/2007	15:58:12	level15	le15	async	stop	115	shell	..
04/23/2007	15:56:19	level15	le15	..	NAS Port re-used	3	..	..
04/23/2007	15:56:16	level15	le15	async	start	..	shell	..
04/23/2007	15:54:07	level15	le15	async	stop	713	shell	..

Step3>如果要记录用户所用的命令，设备端配置为：

aaa new-model
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
line vty 0 4
accounting commands 0 default
accounting commands 1 default
accounting commands 15 default

Step4>然后点击 report and activity 中的 TACACS+ Administration，可以浏览某天某用户的所有命令

Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	NAS-Portname	task_id	NAS-IP-Address	r
04/23/2007	16:12:48	level1	le1	show running-config <cr>	15	shell	tty0	202	218.5.0.40	.
04/23/2007	16:12:46	level1	le1	exit <cr>	0	shell	tty0	201	218.5.0.40	.
04/23/2007	16:02:40	level1	le1	show running-config <cr>	15	shell	tty0	200	218.5.0.40	.
04/23/2007	16:01:56	level1	le1	show ip route <cr>	1	shell	tty0	199	218.5.0.40	.
04/23/2007	16:01:46	level1	le1	exit <cr>	0	shell	tty0	198	218.5.0.40	.
04/23/2007	16:01:36	level1	le1	show running-config <cr>	15	shell	tty0	197	218.5.0.40	.
04/23/2007	16:01:33	level1	le1	show privilege <cr>	1	shell	tty0	196	218.5.0.40	.
04/23/2007	16:01:30	level1	le1	enable <cr>	0	shell	tty0	195	218.5.0.40	.
04/23/2007	16:01:21	level1	le1	exit <cr>	0	shell	tty0	193	218.5.0.40	.
04/23/2007	16:01:19	level1	le1	exit <cr>	0	shell	tty0	192	218.5.0.40	.
04/23/2007	16:01:17	level1	le1	exit <cr>	0	shell	tty0	191	218.5.0.40	.
04/23/2007	16:00:45	level1	le1	exit <cr>	0	shell	tty0	190	218.5.0.40	.
04/23/2007	16:00:43	level1	le1	interface FastEthernet	15	shell	tty0	189	218.5.0.40	.

The End

此手册只介绍了 ACS 的部分基本应用

有误之处 欢迎指正

邱 杨 2007-4-25